



DRAFT INTERNATIONAL STANDARD ISO/IEC DIS 29115

ISO/IEC JTC 1

Secretariat: **ANSI**

Voting begins on
2011-11-23

Voting terminates on
2012-04-23

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОММИСИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Security techniques — Entity authentication assurance framework

Technologies de l'information — Techniques de sécurité — Cadre d'assurance de l'authentification d'entité

ICS 35.040

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/31f022e1-3ba6-4964-849d-3c2bc5fdde6e/iso-iec-29115-2013>

In accordance with the provisions of Council Resolution 21/1986 this DIS is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 21/1986, ce DIS est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/31022e1-3ba6-4964-849d-3c2bc5fdde6e/iso-iec-29115-2013>

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

CONTENTS

	<i>Page</i>
Foreword.....	iii
Summary	iv
1 Scope.....	1
2 Normative references.....	1
2.1 Identical Recommendations International Standards.....	1
2.2 Paired Recommendations International Standards.....	1
2.3 Additional references	1
3 Definitions.....	1
4 Abbreviations.....	3
5 Conventions	4
6 Levels of assurance.....	4
6.1 Level of assurance 1 (LoA1).....	5
6.2 Level of assurance 2 (LoA2).....	5
6.3 Level of assurance 3 (LoA3).....	5
6.4 Level of assurance 4 (LoA4).....	5
6.5 Selecting the appropriate level of assurance.....	6
6.6 LoA mapping and interoperability.....	7
6.7 Exchanging authentication results based on the 4 LoAs.....	7
7 Actors.....	8
7.1 Entity.....	8
7.2 Credential service provider.....	8
7.3 Registration authority.....	8
7.4 Relying party.....	8
7.5 Verifier.....	9
7.6 Trusted third party.....	9
8 Entity authentication assurance framework phases.....	9
8.1 Enrolment phase.....	9
8.1.1 Application and initiation.....	9
8.1.2 Identity proofing.....	10
8.1.3 Identity verification.....	11
8.1.4 Record-keeping/recording.....	11
8.1.5 Registration.....	11
8.2 Credential management phase.....	11
8.2.1 Credential creation.....	11
8.2.2 Credential issuance.....	12
8.2.3 Credential activation.....	12
8.2.4 Credential storage.....	12
8.2.5 Credential suspension, revocation, and/or destruction.....	12
8.2.6 Credential renewal and/or replacement.....	13
8.2.7 Record-keeping.....	13

8.3	Entity authentication phase	13
8.3.1	Authentication	13
8.3.2	Record-keeping	13
9	Management and organizational considerations	14
9.1	Service establishment	14
9.2	Legal and contractual compliance	14
9.3	Financial provisions	14
9.4	Information security management and audit	14
9.5	External service components	14
9.6	Operational infrastructure	15
9.7	Measuring operational capabilities	15
10	Threats and controls	15
10.1	Threats to and controls for the enrolment phase	15
10.1.1	Enrolment phase threats	15
10.1.2	Controls against enrolment phase threats by LoA	15
10.2	Threats to and controls for the credential management phase	18
10.2.1	Credential management threats	18
10.2.2	Controls against credential management phase threats by LoA	19
10.3	Threats to and controls for the authentication phase	22
10.3.1	Authentication phase threats	22
10.3.2	Controls against authentication phase threats by LoA	23
11	Service assurance criteria	26
	Annex A – Privacy and protection of PII	27
	Annex B – Characteristics of a credential	28
	Annex C – Bibliography	29

Foreword

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardisation Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardising telecommunications on a world-wide basis. The World Telecommunication Standardisation Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups that, in turn, produce Recommendations on these topics. The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1. In some areas of information technology that fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29115 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*. The identical text is published as ITU-T Recommendation X.1254.

D R A F T

ITU-T Rec. X.1254 (11/2011)
Draft
<https://standards.iteh.ai/catalog/standards/sist/1254-2011/iso-iec-29115-2011>
3ba6-4964-849d-3c2bec

Summary

Many electronic transactions within or between ICT systems have security requirements which depend upon an understood or specified level of confidence in the identities of the entities involved. Such requirements may include the protection of assets and resources against unauthorized access, for which an access control mechanism might be used, and/or the enforcement of accountability by the maintenance of audit logs of relevant events, as well as for accounting and charging purposes.

This Recommendation | International Standard provides a framework for entity authentication assurance. Assurance within this Recommendation | International Standard refers to the confidence placed in all of the processes, management activities, and technologies used to establish and manage the identity of an entity for use in authentication transactions.

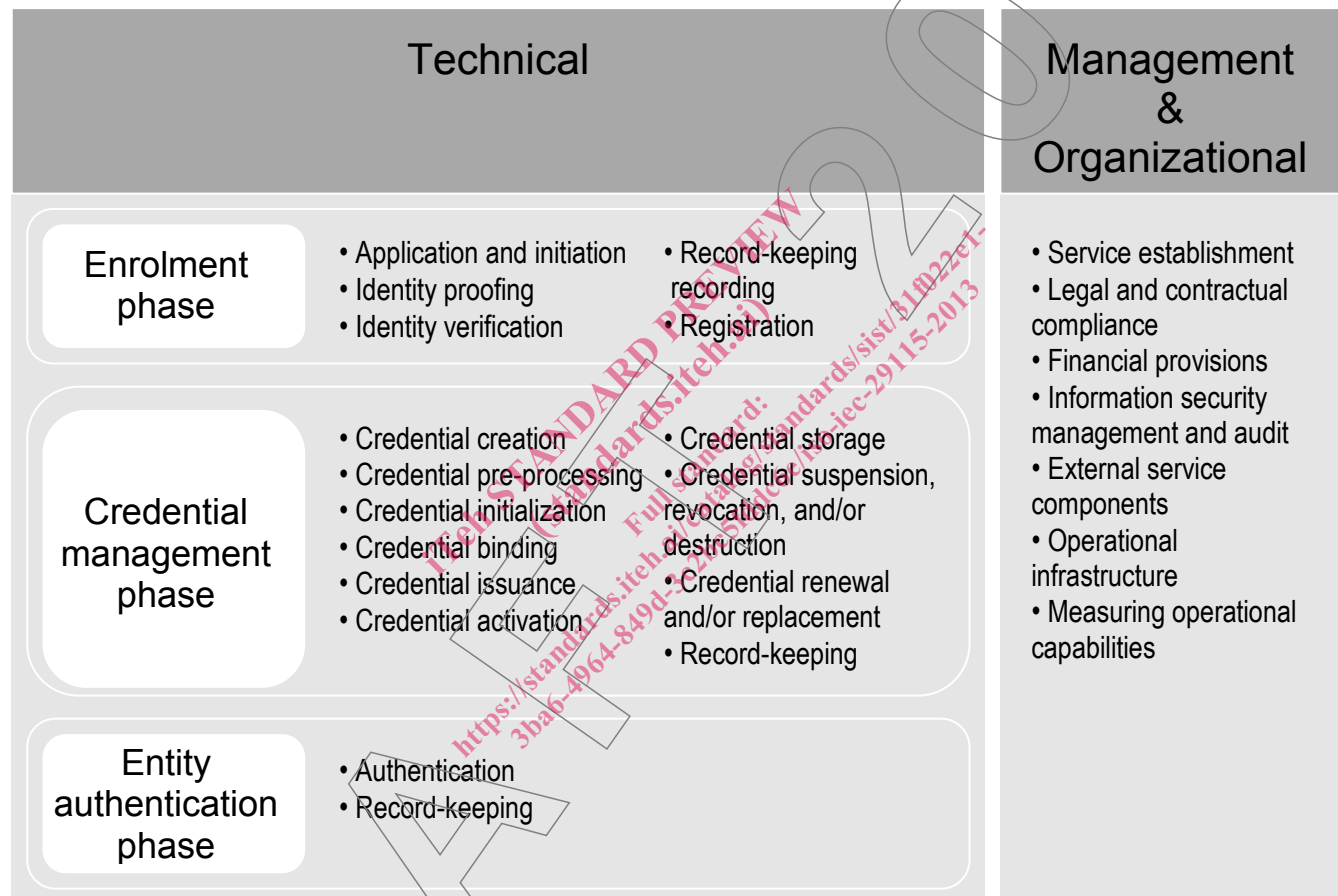


Figure 1 – Overview of the Entity Authentication Assurance Framework

Using four specified Levels of Assurance (LoAs), this Recommendation | International Standard provides guidance concerning control technologies, processes, and management activities, as well as assurance criteria, that should be used to mitigate authentication threats in order to implement the four LoAs. It also provides guidance for the mapping of other authentication assurance schemes to the specified four levels, as well as guidance for exchanging the results of an authentication transaction. Finally, this Recommendation | International Standard provides informative guidance concerning the protection of personally identifiable information (PII) associated with the authentication process.

This Recommendation | International Standard is intended to be used principally by CSPs and by others having an interest in their services (e.g., RPs, assessors and auditors of those services). This Entity Authentication Assurance Framework (EAAF) specifies the minimum technical, management, and process requirements for four LoAs to ensure equivalence among credentials issued by various CSPs. It also provides some additional management and organizational considerations

that affect entity authentication assurance, but it does not set forth specific criteria for those considerations. Relying Parties (RPs) and others may find this Recommendation | International Standard helpful to gain an understanding of what each LoA provides. Additionally, it may be adopted for use within a trust framework to define technical requirements for LoAs. The EAAF is intended for, but not limited to, session-based and document-centric use cases using various authentication technologies. Both direct and brokered trust scenarios are possible, within either bilateral or federated legal constellations.

D R A F T

2011

ITeH STANDARD PREVIEW
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/3ba6-4964-849d-3c2bc5fd1c6e/iso-iec-29115-2013>

Full standard:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/31f022e1-3ba6-4964-849d-3c2bc5fdde6e/iso-iec-29115-2013>

**INTERNATIONAL STANDARD <29115>
ITU-T RECOMMENDATION <X.1254>**

Information technology — Security techniques — Entity authentication assurance framework

1 Scope

This Recommendation | International Standard provides a framework for managing entity authentication assurance in a given context. In particular, it:

- specifies four levels of entity authentication assurance;
- specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance;
- provides guidance for mapping other authentication assurance schemes to the four LoAs;
- provides guidance for exchanging the results of authentication that are based on the four LoAs; and
- provides guidance concerning controls that should be used to mitigate authentication threats.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

None.

2.2 Paired Recommendations | International Standards

None.

2.3 Additional references

None.

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.1 Assertion: Statement made by an entity without accompanying evidence of its validity [ITU-T X.1252].

NOTE - The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with slightly different meanings. For the purposes of this Recommendation | International Standard, an assertion is considered to be a stronger statement than a claim.

3.2 Authentication: Provision of assurance in the claimed identity of an entity [ISO/IEC 18014-2].

3.3 Authentication Factor: Piece of information and process used to authenticate or verify the identity of an entity [ISO/IEC 19790].

NOTE - Authentication factors are divided into four categories:

- something an entity has (e.g., device signature, passport, hardware device containing a credential, private key);
- something an entity knows (e.g., password, PIN);
- something an entity is (e.g., biometric characteristic); or
- something an entity typically does (e.g., behaviour pattern).

3.4 Authentication Protocol: Defined sequence of messages between an entity and a verifier that enables the verifier to corroborate the entity's identity.

3.5 Authoritative Source: Repository which is recognized as being an accurate and up-to-date source of information.

3.6 Claim: Statement that something is the case, without being able to give proof [ITU-T X.1252].

NOTE - The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with slightly different meanings. For the purposes of this Recommendation | International Standard, an assertion is considered to be a stronger statement than a claim.

3.7 Context: Environment with defined boundary conditions in which entities exist and interact [ITU-T X.1252].

3.8 Credential: Set of data presented as evidence of an asserted identity and/or entitlements [ITU-T X.1252].

NOTE - See Annex A for additional characteristics of a credential.

3.9 Credential Service Provider: Trusted actor that issues and/or manages credentials.

NOTE - The Credential Service Provider (CSP) may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or it may issue credentials for its own use.

3.10 Entity: Something that has separate and distinct existence and that can be identified in a context [ITU-T X.1252].

NOTE - For the purposes of this Recommendation | International Standard, entity is also used in the specific case for something that is claiming an identity.

3.11 Entity Authentication Assurance: Degree of confidence reached in the authentication process that the entity is what it claims to be or is expected to be [X.1252].

NOTE - The confidence is based on the degree of confidence in the binding between the entity and the identity that is presented.

3.12 Identifier: One or more attributes that uniquely characterize an entity in a specific context.

3.13 Identity: Set of attributes related to an entity [ISO/IEC 24760].

NOTE - Within a particular context, an identity may have one or more identifiers to allow an entity to be uniquely recognized within that context.

3.14 Identity Proofing: Process by which the Registration Authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance.

3.15 Man-in-the-middle Attack: Attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge.

3.16 Multifactor Authentication: Authentication with at least two independent authentication factors [ISO/IEC 19790].

3.17 Mutual Authentication: Authentication of identities of entities which provides both entities with assurance of each other's identity.

3.18 Non-repudiation: Ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action [X.1252].

3.19 Registration Authority: Trusted actor that establishes and/or verifies and vouches for the identity of an entity to a CSP.

NOTE - The RA may be an integral part of a CSP, or it may be independent from a CSP, but it has a relationship with the CSP.

3.20 Relying Party: Actor that relies on an identity assertion or claim.

- 3.21 Repudiation:** Denial by an entity of a claimed event or action.
- 3.22 Salt:** Non-secret, often random, value that is used in a hashing process.
NOTE - It is also referred to as sand.
- 3.23 Shared Secret:** Secret used in authentication that is known only to the entity and the verifier.
- 3.24 Time Stamp:** Reliable time variant parameter which denotes a point in time with respect to a common reference.
- 3.25 Transaction:** Discrete event between an entity and service provider that supports a business or programmatic purpose.
- 3.26 Trust Framework:** Set of requirements and enforcement mechanisms for parties exchanging identity information.
- 3.27 Trusted Third Party:** Authority or its agent, trusted by other actors with respect to security related activities.
NOTE - A trusted third party is trusted by an entity and/or a verifier for the purposes of authentication.
- 3.28 Validity Period:** Time period during which an identity or credential may be used in one or more transactions.
- 3.29 Verification:** Process of checking information by comparing the provided information with previously corroborated information and the binding to the entity.
- 3.30 Verifier:** Actor that corroborates identity information.
- 3.31 Verify:** Check information by comparing the provided information with previously corroborated information and the binding to the entity.

4 Abbreviations

For the purposes of this International Standard | Recommendation, the following abbreviations apply:

CSP	Credential Service Provider
EAA	Entity Authentication Assurance
EAAF	Entity Authentication Assurance Framework
IdM	Identity Management
ICT	Information and Communications Technology
IP	Internet Protocol
LoA	Level of Assurance
LoAs	Levels of Assurance
MAC	Media Access Control
NPE	Non-Person Entity
PII	Personally-Identifiable Information
PIN	Personal Identification Number
RA	Registration Authority
RP	Relying Party
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security